

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A method for conducting a transaction ~~over a network, the network including between~~ a first system and a second system, the method comprising the steps of:

(a) initiating a transaction session;

(b) comparing a value of the first system with a value of the second system, wherein the value of the first system is associated with a particular transaction session; and

(c) continuing the transaction based on the comparison by

c1) generating an encryption key by the second system if the value of the first system does not match the value of the second system.

2. (original): The method of claim 1 wherein the first system comprises a client system and the second system comprises a server system.

3. (original): The method of claim 2 wherein the value of the client system is in a persistent client-side data file.

4. (original): The method of claim 3 wherein the persistent client-side data file comprises a cookie.

5. (original): The method of claim 4 wherein step b) further comprises:

b1) allowing the server system to compare the value in the cookie with the value in the server system.

6. (currently amended): The method of claim 5-1 wherein if the value in the cookie does not match the value in the server system, continuing step c) further comprises:

- c1) ~~generating an encryption key;~~
- c2) storing a portion of the encryption key in the ~~cookie~~first system; and
- c3) storing the entire encryption key on the ~~server~~second system.

7. (currently amended): The method of claim 6 wherein step c) further comprises:

c4) allowing the ~~server~~second system to transfer encrypted information to the ~~client~~first system; and

c5) allowing the ~~server~~second system to transfer a remaining portion of the encryption key to the ~~client~~first system whereby the encryption key is capable of being utilized by the ~~client~~first system to decrypt the encrypted information.

8. (currently amended): The method of claim 7 wherein step c5) is performed in response to a payment transaction from the ~~client~~first system to the ~~server~~second system.

9. (currently amended): The method of claim 5-6 wherein if the value in the cookie does match the value in the server system, step c) further comprises:

~~c1~~c4) allowing the ~~server~~second system to transfer encrypted information to the ~~client~~first system if the value in the first system matches the value in the second system; and

c2c5) allowing the ~~server-second~~ system to transfer a remaining portion of the encryption key to the ~~client-first~~ system whereby the encryption key is capable of being utilized by the ~~client-first~~ system to decrypt the encrypted information.

10. (currently amended): The method of claim 9 wherein step c2c5) is performed in response to a payment transaction from the ~~client-first~~ system to the ~~server-second~~ system.

11. (currently amended): A system for conducting a transaction ~~over a network, the network including between~~ a first system and a second system, the system comprising:

means for initiating a transaction;

means for comparing a value of the first system with a value of the second system,

wherein the value of the first system is associated with a particular transaction session; and

means for continuing the transaction based on the comparison, wherein the continuing means includes means for generating an encryption key by the second system if the value of the first system does not match the value of the second system.

12. (original): The system of claim 11 wherein the first system comprises a client system and the second system comprises a server system.

13. (original): The system of claim 12 wherein the value of the client system is in a persistent client-side data file.

14. (original): The system of claim 13 wherein the persistent client-side data file comprises a cookie.

15. (original): The system of claim 14 wherein the means for comparing further comprises:

means for allowing the server system to compare the value in the cookie with the value in the server system.

16. (currently amended): The system of claim ~~15-11~~ wherein ~~if the value in the cookie does not match the value in the server system,~~ the means for continuing the transaction further comprises:

~~means for generating an encryption key;~~

~~means for storing a portion of the encryption key in the cookie first system; and~~

~~means for storing the entire encryption key on the server second system.~~

17. (currently amended): The system of claim 16 wherein the means for continuing the transaction further comprises:

~~means for allowing the server second system to transfer encrypted information to the client first system; and~~

~~means for allowing the server second system to transfer a remaining portion of the encryption key to the client first system whereby the encryption key is capable of being utilized by the client first system to decrypt the encrypted information.~~

18. (currently amended): The system of claim 17 wherein the means for allowing the ~~server second system~~ to transfer a remaining portion of the encryption key is performed in response to a payment transaction from the ~~client first system~~ to the ~~server second system~~.

19. (currently amended): The system of claim ~~15-16~~ wherein ~~if the value in the cookie does match the value in the server system~~, the means for continuing the transaction further comprises:

means for allowing the ~~server-second~~ system to transfer encrypted information to the ~~client-first~~ system if the value in the first system matches the value in the second system; and

means for allowing the ~~server-second~~ system to transfer a remaining portion of the encryption key to the ~~client-first~~ system whereby the encryption key is capable of being utilized by the ~~client-first~~ system to decrypt the encrypted information.

B 1 20. (currently amended): The system of claim 19 wherein the means for allowing the ~~server-second~~ system to transfer a remaining portion of the encryption key is performed in response to a payment transaction from the ~~client-first~~ system to the ~~server-second~~ system.

21. (currently amended): A computer readable medium containing program instructions for conducting a transaction ~~over a network, the network including between~~ a first system and a second system, the program instructions comprising the steps of:

- (a) initiating a transaction;
- (b) comparing a value of the first system with a value of the second system, wherein the value of the first system is associated with a particular transaction session; and
- (c) continuing the transaction based on the comparison by:
 - (c1) generating an encryption key by the second system if the value of the first system does not match the value of the second system.

22. (original): The computer readable medium of claim 21 wherein the first system comprises a client system and the second system comprises a server system.

23. (original): The computer readable medium of claim 22 wherein the value of the client system is in a persistent client-side data file.

24. (original): The computer readable medium of claim 23 wherein the persistent client-side data file comprises a cookie.

25. (original): The computer readable medium of claim 24 wherein step b) further comprises:

b1) allowing the server system to compare the value in the cookie with the value in the server system.

26. (currently amended): The computer readable medium of claim ~~25~~ 21 wherein if the value in the cookie does not match the value in the server system, step c) further comprises:

~~c1) generating an encryption key;~~

c2) storing a portion of the encryption key in the ~~cookie~~ first system; and

c3) storing the entire encryption key on the ~~server~~ second system.

27. (currently amended): The computer readable medium of claim 26 wherein step c) further comprises:

c4) allowing the ~~server~~ second system to transfer encrypted information to the ~~client~~ first system; and

c5) allowing the ~~server-second~~ system to transfer a remaining portion of the encryption key to the ~~client-first~~ system whereby the encryption key is capable of being utilized by the ~~client-first~~ system to decrypt the encrypted information.

28. (currently amended): The computer readable medium of claim 27 wherein step c5) is performed in response to a payment transaction from the ~~client-first~~ system to the ~~server-second~~ system.

29. (currently amended): The computer readable medium of claim ~~25-26~~ wherein if the value in the cookie does match the value in the server system, step c) further comprises:

b1
c1c4) allowing the ~~server-second~~ system to transfer encrypted information to the client system if the value in the first system matches the value in the second system,; and

c2c5) allowing the ~~server-second~~ system to transfer a remaining portion of the encryption key to the ~~client-first~~ system whereby the encryption key is capable of being utilized by the ~~client-first~~ system to decrypt the encrypted information.

30. (currently amended): The computer readable medium of claim 29 wherein step ~~c2c5~~) is performed in response to a payment transaction from the ~~client-first~~ system to the ~~server second~~ system.